Memorandum Of Dec. 10, 2004 Telecom

As noted, this is the attempted clarification of the "Identity Theft" prevention component in Claim 6.

It is respectfully submitted that neither of the Ginter patents cited contain any component applicable to preventing identity theft.

In a nutshell, this invention serves to prevent Identity Theft by recording and digitizing the distinct voice patterns of an individual and storing the digitized voice pattern in a database. If anyone other than the "genuine" person would attempt to obtain credit under that name, the credit issuer, through "FICO" or other credit reporting agencies, is directed to the "VoiceGuard My ID" database and the person seeking credit is requested to speak their name. Being they are not the original party, their voiceprint will not match and they would be exposed as a person attempting to steal the identity of the original party. This person would then be taken into custody and the original party would be notified.

The "SHIFT" Claim 6, identity theft prevention component (operated as "VoiceGuard My ID") functions in the following manner:

The "VoiceGuard My ID" Registration Process

A prospective Client would go to the "VoiceGuard My ID" web site and would be informed in detail of how the "VoiceGuard My ID" system operates to protect them from having their identity stolen.

If they elect to sign up, they would read directions on how they must fill out an enrollment form with basic personal information and pay for the "VoiceGuard My ID" service with a personal Credit Card.

One of the following (or additional) processes would then be employed to verify that the prospective Client is the "genuine" person that they purport to be.

1. They would be required to supply the name/address of the bank and a number of one of their bank accounts at the bank they will be going to. The client would then receive an 800 number and a code number and would be instructed to go to their bank and to request that a bank officer assist them in registering their voice with "VoiceGuard My ID".

   At the bank they then request a Bank official to call the "800" # and to provide the "code number". At that point, a "VoiceGuard My ID" representative asks the Bank Officer to confirm that the individual is the person they are asserting that they are. If the Identity is positively confirmed by the Bank Official, the person is given the phone and requested to say their name and address and a series of words or numerals (used as a PIN) and their Social Security number and to then repeat the same information a second time.

2. The prospective Client would go to the web site and enroll as described above. The Client would be provided with an 800 # and a "code number" and would be instructed to fax or mail a copy of a picture driver's license to that number. They would also be informed that a "VoiceGuard My ID" representative would call their home phone at a random time so as to confirm that they are the person on the picture driver's license.

The "VoiceGuard My ID" representative would record and digitize the Client's voice and store it in the "VoiceGuard My ID" database.

An existing "voice digitization" system is to be licensed and employed to digitize the name, address, PIN and Social Security number of the Client and the digitized sample is then entered into a secure "VoiceGuard My ID" database.

The "VoiceGuard My ID" Identity Protection Process

The Client's digitized voice sample is then "flagged" in the databases of "Fico" (Fair Isaacs) and similar type credit databases. Whenever anyone attempts to obtain any form of new credit under that name, the "flag" in the credit information system's databases direct the request to the "VoiceGuard My ID" database.

The "VoiceGuard My ID" database then provides a "different code number" and "800 Number" and directs that the Credit Issuer have the person call the 800 number and when requested for the "code number" to enter it, at which time the "VoiceGuard My ID" database system searches for that specific "code number" from which it takes a "COPY" of the genuine registered Client's digitized voice and places it in a separate disposable "module".

That "module" then requests the credit applicant to say their name, address, Social Security number and PIN, which is then instantly digitize and compared to the "genuine" voiceprint of the "genuine" person contained in the "module" . If the digitized voices match, then "VoiceGuard My ID" informs the Credit Issuer that the credit applicant is the person they purport to be and that credit may be given if all else warrants.

If the digitized voice does not match the voice of record, then the Credit Issuer is informed that an "Identity Theft" is being attempted and to detain the party and to call their security personnel or the police.

The "VoiceGuard My ID" system then contacts the registered Client and informs them of the attempt and provides them with the phone number of the Credit Issuer and recommends the registered Client determine if they know the person who attempted to steal their Identity in order to give the registered Client the final say of if they want the person prosecuted, this in the event that it was a family member that they may not want prosecuted. This information of attempted Identity thefts are then stored in a separate and different database for security reasons.

The "VoiceGuard My ID" Module

The "VoiceGuard My ID" database is kept secure at all times. There is no direct Internet access to the prime "VoiceGuard My ID" database. Hence the prime database can never be available to Hackers.

When a verification request comes to an Internet access "VoiceGuard My ID" computer, that computer, after going through a number of "firewalls" employs the "code number" to request a "COPY" of the particular Client's sample voice, which is placed in a special "module" that also contains a voice digitization mechanism, which is then used for the voiceprint verification process as described above.

Once the "module" completes a comparison process, the results are then sent back to a second and totally separate "VoiceGuard My ID" database that is accessible only by the name of the Client, the social security number and PIN first being deleted. Once this process is complete, the "module" self destructs.

This faction of the "VoiceGuard My ID" process is specifically designed and intended to prevent unauthorized persons from obtaining any form of "NEW" credit under a registered Client's name.

Optional Credit Card Security Faction

A second available process of "VoiceGuard My ID" is designed to protect the theft and misuse of credit cards.

With this process, a Client would determine a purchase limit for their credit cards and/or a specific number of high priced purchases that could be made with their card within a twelve (12) hour period. If the Client selects a Two Hundred ($200.00) Dollar (or any given amount) limit on any credit card purchase, that specific amount would be registered, by virtue of a "flag" on the persons name at their credit card issuer database.

In the event the card was stolen or was being misused for purchases over the specified amount, the credit card issuer database "flag" would contact the "VoiceGuard My ID" database and the voiceprint verification process described above would be employed to verify whether or not the party was the "genuine" person entitled to use the card.

This faction of "VoiceGuard My ID" would serve to prevent any extreme loss if a credit card was stolen or misused.

The "SHIFT" System

It is respectfully submitted that the Ginter patents do not have any portion of the SHIFT system. The SHIFT system is the only system that changes the "Vendor Take From" system to a "Cardholder Pay To" system and which prevents anyone from being able to Hack and steal credit card numbers over the Internet.

Ginter requires a number of complex electronic components to be in a person's control and transmits information, including credit card numbers over the Internet. The SHIFT unit is battery operated and requires no other equipment in the possession and control of a user other than a telephone line and does not transmit information or credit card numbers over the Internet.

The Ginter system employs transmissions over the Internet. The SHIFT unit transmits information from the person to the computer database of the specific credit card issuer over a telephone line directly from the individual to the database and does not transmit any form of information over the Internet.

With SHIFT, a person may shop over the Internet. When the person makes a purchase, they do not provide credit card numbers to the merchant. They only provide their name, address and phone number to the merchant.

With SHIFT, the merchant gives the shopper the merchants "deposit only account number" (a bank account number that only deposits can be made to – does not allow withdrawals). The merchant does not ship the purchased item until he is notified that a payment has been made to this account by the shopper.

Once the shopper is given the merchant deposit only account number and an Invoice number, the shopper then uses the SHIFT battery operated unit to call the credit card issuer computer database over a private telephone line, to instruct that database to make a specified amount payment to the merchants "deposit only" account number in payment for the Invoice number.

The only parties having access to the shopper's credit card number are the shopper and the credit card issuer. Being the credit card number is never given over the Internet, the number is never available to Hackers where it can be stolen or misused.

Greater details of other factions of the SHIFT system are spelled out in the original application.